入侵偵測防禦系統資通安全檢測技術規範

第6點修正總說明

為使本技術規範對目前市場上產品有更精確之技術要求，及參酌本會101年5月29日召開「防火牆及入侵偵測防禦系統資通安全檢測技術規範」實機測試紀錄研討會議之檢測報告，爰修訂入侵偵測防禦系統資通安全檢測技術規範第6點技術要求部分規定，主要修正重點分述如下：

1. 6.4.1.安全功能管理-作部分文字修正。
2. 6.4.1.5線上更新-修正測試環境、測試方法及標準。
3. 6.4.2壓力測試-刪除進行壓力測試時，不能發生封包遺失之要求

入侵偵測防禦系統資通安全檢測技術規範

第6點修正對照表

| 修正規定 | 現行條文 | 說明 |
| --- | --- | --- |
| 6.4.1.3.2. 測試方法及標準  (1) 由測試平台連線至待測物，確認待測物是否需要通行碼才可進行設定，待測物應須輸入正確通行碼才可進行管理設定。  (2) 嘗試輸入錯誤通行碼，待測物是否檢查當超過最大錯誤次數時，會封鎖管理介面一段時間，避免遭受攻擊。 | 6.4.1.3.2. 測試方法及標準  (1) 由測試平台連線至待測物，確認待測物是否需要密碼才可進行設定，待測物應須輸入正確密碼才可進行管理設定。  (2) 嘗試輸入錯誤密碼，待測物是否檢查當超過最大錯誤次數時，會封鎖管理介面一段時間，避免遭受攻擊。 | 將密碼用語統一改為通行碼，避免混淆。 |
| 6.4.1.5. 線上更新  6.4.1.5.1. 測試環境  (1) 測試平台：可供測試人員連線至待測物之終端設備。  (2) 網路連接線：乙太網路線或光纖纜線。  (3) 連接待測物、測試平台與網際網路如圖3。  (4) 開啟待測物之自動線上更新功能。  6.4.1.5.2. 測試方法及標準  待測物應至少每天一次自動進行線上入侵攻擊特徵碼之更新。 | 6.4.1.5. 線上更新  6.4.1.5.1. 測試環境  (1) 測試平台：可供測試人員連線至待測物之終端設備。  (2) 網路連接線：乙太網路線或光纖纜線。  (3) 連接待測物、測試平台與網際網路如圖3。  (4) 開啟待測物之線上更新功能（自動更新或手動更新）。  6.4.1.5.2. 測試方法及標準  (1) 以測試平台開啟待測物之自動更新功能，確認待測物可自動更新掃毒引擎與特徵碼。  (2) 以測試平台開啟待測物之手動更新功能，並設定每5分鐘自動更新，確認待測物可自動更新掃毒引擎與病毒特徵碼。  (3) 以測試平台開啟待測物之手動更新功能，並設定每60分鐘自動更新，確認待測物可自動更新掃毒引擎與病毒特徵碼。  (4) 以測試平台開啟待測物之手動更新功能，並設定每周一、三及五之凌晨5點自動更新，確認待測物可自動更新掃毒引擎與病毒特徵碼。 | 原條文要求待測物必須支援客製化更新頻率與時間，實無必要。考量整體安全性與參考國際大廠現行做法，將條文修改為每日至少進行一次特徵碼之自動更新。 |
| 6.4.2.1.2. 測試方法及標準  測試平台建立自A埠經待測物至B埠之網路連線後，傳送不同大小之封包。當待測物所負荷的吞吐量達到其規格說明之最大值時，待測物安全功能應正常運作。 | 6.4.2.1.2. 測試方法及標準  測試平台建立自A埠經待測物至B埠之網路連線後，傳送不同大小之封包。當待測物所負荷的吞吐量達到其規格說明之最大值時，不能發生封包遺失且待測物安全功能應正常運作。 | 進行壓力測試時，待測物丟棄部分封包屬正常功能，故刪除此要求。 |